AFRL-OSR-VA-TR-2015-0128

PROVABLE SECURITY OF COMMUNICATION FOR PROTECTING INFORMATION

Paul Cuff
TRUSTEES OF PRINCETON UNIVERSITY

06/01/2015
Final Report

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ RTC
Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
26-05-2015	Final Report	1 July 2012 - 30 June 2015

4. TITLE AND SUBTITLE
Provable Security of Communication for Protecting Information Flow in Distributed Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-12-1-0196

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Dr. Paul Cuff

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Princeton University
35 Olden Street
Princeton, NJ 08544

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
A

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This report includes a detailed summary of the highlights of the research project during the final year of funding as well as a complete report on the publications and results produced during the entire duration of the project (four journal papers and 24 conference publications). There are also three research papers under review and two in preparation, which are not listed in this report.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		7	Paul Cuff
					19b. TELEPHONE NUMBER *(Include area code)* 609-258-7946

Reset

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

Final Report

Grant Title: Provable Security of Communication for Protecting Information Flow in Distributed Systems

Grant #: FA9550-12-1-0196

Principle Investigator: Dr. Paul Cuff

Reporting Period: 1 July 2012 to 30 June 2015

Abstract:

This report includes a detailed summary of the highlights of the research project during the final year of funding as well as a complete report on the publications and results produced during the entire duration of the project. There are also three research papers under review and two in preparation, which are not listed in this report.

Report for final year:

Annual accomplishments (final one year):

Secret key agreement with Gaussian sources: Complementary to this project is the production of secure digital resources that are used for secure encoding of signals. Within this space is physical layer security and, in particular, secret key agreement. The secret key agreement problem where correlated observations are used to generate a key, with the use of limited public communication, has been solved in the literature for two nodes with i.i.d. sources, to the point of an information theoretic statement that requires optimization. Explicit formulas have been derived in the literature for the important Gaussian case. We have provided an explicit solution for vector Gaussian sources and extended to arbitrary stationary Gaussian sources. This is one of the most relevant cases in practice, and the solution has a nice water-filling interpretation over the spectrum. Furthermore, the analysis provides new insights into the tensorization of extremal mutual information quantities, which have been of recent interest in the community. Additionally, we have derived fundamental limits for secret key agreement among more than two nodes with a single communicator, for general distributions. This has been submitted as a journal paper.

Secure source coding with side information or a helper: We developed schemes for utilizing side-information in a secure signal encoding protocol. Two settings have been studied---one where the side-information is at the decoder, and another where a helper encodes the side-information. In some situations (with no causal disclosure), the side-

information can allow us to completely obscure the signal from the eavesdropper.

Joint source-channel coding: While most of this project deals with secure source encoding (compression), we have shown that if source coding and channel coding are designed jointly and used to transmit information across a noisy channel they can perform better than separate designs connected together. This differs from the source-channel separation theorem for point-to-point non-secure communication.

Common information for Gaussian variables: Wyner defined an important information quantity called common information which plays an important role in secure compression. Recently, an explicit formula for the scalar Gaussian common information was derived in the literature. We provided the vector Gaussian formula. The proof technique extends to more complicated information theoretic regions than common information (such as those in our theorem statements).

Differential Privacy and Mutual Information: A recent popular notion of database privacy is "differential privacy." We have discovered a fundamental connection between this metric of privacy and a mutual information quantity. This connection allows a deep understanding of what the metric is actually assuring.

Professional Human Training Opportunities (final one year):

Curt Schieler completed his Ph.D thesis and degree based on this project.

Two women have played major roles in this research project over the past year.

Seven Ph.D students conducted research as part of this project.

Ph.D. students C. Song, S. Satpathy, and J. Liu, each advised by the P.I., attended the 2014 North American School of Information Theory. They attended lectures and presented posters explaining their recent contributions toward information theoretic secrecy of signals.

Three undergraduates conducted research projects with the P.I. Aaron Himelman, worked on developing a new ranking algorithm for sports teams. Michael Freyberger worked on zero-delay source coding for secrecy. Timothy Seah implemented a novel LASSO optimization algorithm for pitch and instrument detection. Each of these students gave a presentation and wrote a report on the work.

Disseminated to communities of interest (final one year):

Two IEEE journal articles have been published in the last year, related to this project. Three more journal articles from this work are under review.

The P.I. gave a three hour tutorial on the topic of this project at SPCOM 2014. The P.I. has also been invited to give four other conference talks on the topic.

Additionally, five other conference presentations on the topic of this project have been given by Ph.D. students during the past year.

Impact on the development of the principal discipline of the project (final one year):

The primary way that the fields of security and information theory are affected by the recent developments of this project is by filling in a missing piece of crucial understanding. We can roughly divide the field up into four main categories: first, channel coding (the conversion of noisy and imperfect physical resources into ideal digital resources); second, source coding (the conversion of information signals into digital representations); and third and fourth, the secure versions of the first two. This project adds crucial understanding to the fourth category, secure source coding. This work is very different from previous approaches in the field, and the P.I. expects that this project may ultimately be viewed as the right way to approach this problem. For one thing, we have shown this approach to be a generalization of the standard previous approach.

This work also contributes the likelihood encoder technique, which is a generally useful in the field of information theory. It is already beginning to be used by others in the field.

Secret key agreement has been an important and well studied topic. Our solution for the stationary Guassian case brings this closer to practical applications.

Impact on other disciplines (final one year):

The simplified understanding of causal secrecy as synthesizing a memoryless channel (published in a journal article this year) puts the technology in a position to be utilized for distributed control. We have begun to make this claim concrete. Potentially this technology will become a staple for efficiently using digital resources in a secure control system, in such a way that is easy to analyze.

Also, in the field of control, our bounds on convergence time for distributed consensus are the leading universal bounds for this actively studied problem.

The differential privacy discoveries of this project will affect the way differential privacy is understood and used in other fields such as computer science, statistics, and machine learning.

Impact on society beyond science and technology (final one year):

Secure encoding of information enables the design of systems of great importance to society. Upon applying this theory, important infrastructure used ubiquitously, such as communication networks, power grids, etc., can be made more secure again malicious attacks.

Archival Publications supported by this project (final one year---journal articles in bold):

1) E. Song, P. Cuff, V. Poor, "Joint Source-Channel Secrecy using Hybrid Coding," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
2) S. Satpathy and P. Cuff, "Gaussian Secure Source Coding and Wyner's Common Information," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
3) J. Liu, P. Cuff, S. Verdu, "Secrecy Key Generation with One Communicator and a One-Shot Converse via Hypercontractivity," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
4) J. Liu, P. Cuff, S. Verdu, "One-shot Mutual Covering Lemma and Marton's Inner Bound with a Common Message," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
5) J. Liu, P. Cuff, S. Verdu, "Resolvability in E-gamma with applications to Lossy Compression and Wiretap Channels," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
6) **S. Shang, P. Cuff, P. Hui, S. Kulkarni, "An Upper Bound on the Convergence Time for Quantized Consensus of Arbitrary Static Graphs," IEEE Trans. on Automatic Control, 60(4):1127-32, April, 2015.**
7) **C. Schieler and P. Cuff, "Rate-Distortion Theory for Secrecy Systems," IEEE Trans. on Inf. Theory, 60(12):7584-605, Dec., 2014.**
8) E. Song, P. Cuff, V. Poor, "A Rate-Distortion Based Secrecy System with Side Information at the Decoders," Proc. of the Allerton Conference on Communication, Control, and Computing, Oct. 2014.
9) S. Satpathy and P. Cuff, "Secure Coordination with a Two-Sided Helper," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2014.
10) E. Song, P. Cuff, V. Poor, "The Likelihood Encoder for Lossy Source Compression," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2014.
11) C. Schieler and P. Cuff, "The Henchman Problem: Measuring Secrecy by the Minimum Distortion in a List," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2014.
12) J. Liu, P. Cuff, S. Verdu, "Key Capacity with Limited One-Way Communication for Product Sources," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2014.
13) S. Shang, Y. Hui, P. Hui, P. Cuff, S. Kulkarni, "The Application of Differential Privacy for Rank Aggregation: Privacy and Accuracy," Proc. of the Int'l. Conf. on Information Fusion, July, 2014.

Complete report:

Research highlights:

The journal publications produced by this project encapsulate the most exciting results of this project, in particular 7) and 16) below (three other journal papers are currently under review). These articles have the potential to become groundwork for a new theory of secure source coding. Others in the information theory field are beginning to take interest. The novelty is that it is a theory about compressing and encoding information in a secure way, which can be employed at the end-points of the network rather than the physical layer if desired. It differs from other work on secure source coding in that security is measured by what the eavesdropper can do with the obtained information, in a distortion or competitive sense. The content of 7) outlines the fundamental tradeoffs between security resources expended and performance. We were able to develop this theory with definitions much stronger than originally anticipated. Furthermore, to our surprise, we were able to show rigorously that this is a richer and more general theory than the traditional approach, which uses entropy as a measure of security (referred to as "equivocation").

This main contribution, described in the previous paragraph, has consequences beyond the field of information theory and communication. Since the theory can handle signals that come from sensors, it is a relevant approach for encoding signals that are used for distributed control. Thus, the project outputs are bridging across fields and addressing challenges in control.

The article 16) is a new communication tool for synthesizing genuine random noise at a remote location that is correlated with local information. This technique plays a fundamental role in secure encoding of information (such as sensor measurements). It is also a useful tool for coordination among various nodes. This result has influenced the field by inspiring several follow on projects by other groups at other institutions.

An analysis tool emerged from this research project, which we refer to as the "likelihood encoder." We have spoken about this tool at conferences (10 and 18 below), and a journal paper is under review. It turns out to be broadly applicable for source coding. This tool allows for cleaner, more powerful proofs and has the potential to broadly impact the techniques used in information theory.

Archival publications supported by this project (journal articles in bold):

1) E. Song, P. Cuff, V. Poor, "Joint Source-Channel Secrecy using Hybrid Coding," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
2) S. Satpathy and P. Cuff, "Gaussian Secure Source Coding and Wyner's Common Information," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
3) J. Liu, P. Cuff, S. Verdu, "Secrecy Key Generation with One Communicator and a One-Shot Converse via Hypercontractivity," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
4) J. Liu, P. Cuff, S. Verdu, "One-shot Mutual Covering Lemma and Marton's Inner Bound with a Common Message," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
5) J. Liu, P. Cuff, S. Verdu, "Resolvability in E-gamma with applications to Lossy Compression and Wiretap Channels," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
6) **S. Shang, P. Cuff, P. Hui, S. Kulkarni, "An Upper Bound on the Convergence Time for Quantized Consensus of Arbitrary Static Graphs," IEEE Trans. on Automatic Control, 60(4):1127-32, April, 2015.**
7) **C. Schieler and P. Cuff, "Rate-Distortion Theory for Secrecy Systems," IEEE Trans. on Inf. Theory, 60(12):7584-605, Dec., 2014.**
8) E. Song, P. Cuff, V. Poor, "A Rate-Distortion Based Secrecy System with Side Information at the Decoders," Proc. of the Allerton Conference on Communication, Control, and Computing, Oct. 2014.
9) S. Satpathy and P. Cuff, "Secure Coordination with a Two-Sided Helper," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2014.
10) E. Song, P. Cuff, V. Poor, "The Likelihood Encoder for Lossy Source Compression," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2014.
11) C. Schieler and P. Cuff, "The Henchman Problem: Measuring Secrecy by the Minimum Distortion in a List," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2014.
12) J. Liu, P. Cuff, S. Verdu, "Key Capacity with Limited One-Way Communication for Product Sources," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2014.
13) S. Shang, Y. Hui, P. Hui, P. Cuff, S. Kulkarni, "The Application of Differential Privacy for Rank Aggregation: Privacy and Accuracy," Proc. of the Int'l. Conf. on Information Fusion, July, 2014.
14) **E. Song, E. Soljanin, P. Cuff, V. Poor, K. Guan, "Rate-Distortion-Based Physical Layer Secrecy in Multimode Fiber," IEEE Trans. on Communications, 62(3):1080-90, March, 2014.**
15) S. Shang, T. Wang, P. Cuff, S. Kulkarni, "Beyond Personalization and Anonymity: Toward a Group-Based Recommender System," Proc. Of Symp. on Applied Computing (SAC), March, 2014.

16) P. Cuff, "Distributed Channel Synthesis," IEEE Trans. on Inf. Theory, 59(11):7071-96, Nov., 2013.

17) C. Schieler and P. Cuff, "A Connection between Good Rate-distortion Codes and Backward DMCs," Proc. of IEEE Inf. Theory Workshop (ITW), Sept., 2013.

18) P. Cuff, E. Song, "The Likelihood Encoder for Source Coding," Proc. of IEEE Inf. Theory Workshop (ITW), Sept., 2013.

19) S. Satpathy and P. Cuff, "Secure Cascade Channel Synthesis," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2013.

20) E. Song, P. Cuff, V. Poor, "A Bit of Secrecy for Gaussian Source Compression," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2013.

21) C. Schieler and P. Cuff, "Rate-Distortion Theory for Secrecy Systems," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2013.

22) S. Shang, P. Cuff, P. Hui, and S. Kulkarni, "An Upper Bound on the Convergence Time for Quantized Consensus," Proceedings of IEEE INFOCOM, April, 2013.

23) P. Cuff, "Optimal Equivocation in Secrecy Systems – A Special Case of Distortion-based Characterization," Proc. of the Information Theory and Applications Workshop (ITA), February, 2013.

24) C. Schieler, E. Song, P. Cuff, and V. Poor, "Source-Channel Secrecy with Causal Disclosure," Proc. of the Allerton Conference on Communication, Control, and Computing, Oct. 2012.

25) T. Wang, J. Sturm, P. Cuff, S. Kulkarni, "Condorcet Voting Methods Avoid the Paradoxes of Voting Theory," Proc. of the Allerton Conference on Communication, Control, and Computing, Oct. 2012.

26) S. Shang, S. Kulkarni, P. Cuff, P. Hui, "A Random Walk Based Model Incorporating Social Information for Recommendations," Proc. of the IEEE Machine Learning for Signal Processing Workshop, September, 2012.

27) C. Schieler and P. Cuff, "Secrecy is Cheap if the Adversary Must Reconstruct," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2012.

28) S. Shang, P. Cuff, S. Kulkarni, and P. Hui, "An Upper Bound on the Convergence Time for Distributed Binary Consensus," Proc. of the Int'l. Conf. on Information Fusion, July, 2012.

1.

1. Report Type

Final Report

Primary Contact E-mail
Contact email if there is a problem with the report.

cuff@princeton.edu

Primary Contact Phone Number
Contact phone number if there is a problem with the report

609-258-7946

Organization / Institution name

Princeton University

Grant/Contract Title
The full title of the funded effort.

Provable Security of Communication for Protecting Information Flow in Distributed Systems

Grant/Contract Number
AFOSR assigned control number. It must begin with "FA9550" or "F49620" or "FA2386".

FA9550-12-1-0196

Principal Investigator Name
The full name of the principal investigator on the grant or contract.

Paul Cuff

Program Manager
The AFOSR Program Manager currently assigned to the award

Tristan Nguyen

Reporting Period Start Date

07/01/2012

Reporting Period End Date

06/30/2015

Abstract

This report includes a detailed summary of the highlights of the research project during the final year of funding as well as a complete report on the publications and results produced during the entire duration of the project (four journal papers and 24 conference publications). There are also three research papers under review and two in preparation, which are not listed in this report.

The journal publications produced by this project encapsulate the most exciting results of this project, in particular 7) and 16) listed in the report (and the three other journal papers currently under review). These articles have the potential to become groundwork for a new theory of secure source coding. Others in the information theory field are beginning to take interest. The novelty is that it is a theory about compressing and encoding information in a secure way, which can be employed at the end-points of the network rather than the physical layer if desired. It differs from other work on secure source coding in that security is measured by what the eavesdropper can do with the obtained information, in a distortion or competitive sense. The content of 7) outlines the fundamental tradeoffs between security resources expended and performance. We were able to develop this theory with definitions much stronger than originally anticipated. Furthermore, to our surprise, we were able to show rigorously that this is a richer and more general theory than the traditional approach, which uses entropy as a measure of security (referred to as

"equivocation").

This main contribution, described in the previous paragraph, has consequences beyond the field of information theory and communication. Since the theory can handle signals that come from sensors, it is a relevant approach for encoding signals that are used for distributed control. Thus, the project outputs are bridging across fields and addressing challenges in control.

The article 16) is a new communication tool for synthesizing genuine random noise at a remote location that is correlated with local information. This technique plays a fundamental role in secure encoding of information (such as sensor measurements). It is also a useful tool for coordination among various nodes. This result has influenced the field by inspiring several follow on projects by other groups at other institutions.

An analysis tool emerged from this research project, which we refer to as the "likelihood encoder." We have spoken about this tool at conferences (10 and 18 in the report), and a journal paper is under review. It turns out to be broadly applicable for source coding. This tool allows for cleaner, more powerful proofs and has the potential to broadly impact the techniques used in information theory.

Distribution Statement

This is block 12 on the SF298 form.

Distribution A - Approved for Public Release

Explanation for Distribution Statement

If this is not approved for public release, please provide a short explanation. E.g., contains proprietary information.

SF298 Form

Please attach your SF298 form. A blank SF298 can be found here. Please do not password protect or secure the PDF The maximum file size for an SF298 is 50MB.

AFD-070820-035.pdf

Upload the Report Document. File must be a PDF. Please do not password protect or secure the PDF . The maximum file size for the Report Document is 50MB.

Final Report.pdf

Upload a Report Document, if any. The maximum file size for the Report Document is 50MB.

Archival Publications (published) during reporting period:

1) E. Song, P. Cuff, V. Poor, "Joint Source-Channel Secrecy using Hybrid Coding," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
2) S. Satpathy and P. Cuff, "Gaussian Secure Source Coding and Wyner's Common Information," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
3) J. Liu, P. Cuff, S. Verdu, "Secrecy Key Generation with One Communicator and a One-Shot Converse via Hypercontractivity," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
4) J. Liu, P. Cuff, S. Verdu, "One-shot Mutual Covering Lemma and Marton's Inner Bound with a Common Message," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
5) J. Liu, P. Cuff, S. Verdu, "Resolvability in E-gamma with applications to Lossy Compression and Wiretap Channels," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), June, 2015.
6) S. Shang, P. Cuff, P. Hui, S. Kulkarni, "An Upper Bound on the Convergence Time for Quantized Consensus of Arbitrary Static Graphs," IEEE Trans. on Automatic Control, 60(4):1127-32, April, 2015.
7) C. Schieler and P. Cuff, "Rate-Distortion Theory for Secrecy Systems," IEEE Trans. on Inf. Theory, 60(12):7584-605, Dec., 2014.
8) E. Song, P. Cuff, V. Poor, "A Rate-Distortion Based Secrecy System with Side Information at the Decoders," Proc. of the Allerton Conference on Communication, Control, and Computing, Oct. 2014.
9) S. Satpathy and P. Cuff, "Secure Coordination with a Two-Sided Helper," Proc. of IEEE Int'l. Symp. on Inf. Theory (ISIT), July, 2014.
10) E. Song, P. Cuff, V. Poor, "The Likelihood Encoder for Lossy Source Compression," Proc. of IEEE Int'l.

Symp. on Inf. Theory (ISIT), July, 2014.
11) C. Schieler and P. Cuff, “The Henchman Problem: Measuring Secrecy by the Minimum Distortion in a List,” Proc. of IEEE Int’l. Symp. on Inf. Theory (ISIT), July, 2014.
12) J. Liu, P. Cuff, S. Verdu, “Key Capacity with Limited One-Way Communication for Product Sources,” Proc. of IEEE Int’l. Symp. on Inf. Theory (ISIT), July, 2014.
13) S. Shang, Y. Hui, P. Hui, P. Cuff, S. Kulkarni, “The Application of Differential Privacy for Rank Aggregation: Privacy and Accuracy,” Proc. of the Int’l. Conf. on Information Fusion, July, 2014.
14) E. Song, E. Soljanin, P. Cuff, V. Poor, K. Guan, “Rate-Distortion-Based Physical Layer Secrecy in Multimode Fiber,” IEEE Trans. on Communications, 62(3):1080-90, March, 2014.
15) S. Shang, T. Wang, P. Cuff, S. Kulkarni, “Beyond Personalization and Anonymity: Toward a Group-Based Recommender System,” Proc. Of Symp. on Applied Computing (SAC), March, 2014.
16) P. Cuff, “Distributed Channel Synthesis,” IEEE Trans. on Inf. Theory, 59(11):7071-96, Nov., 2013.
17) C. Schieler and P. Cuff, “A Connection between Good Rate-distortion Codes and Backward DMCs,” Proc. of IEEE Inf. Theory Workshop (ITW), Sept., 2013.
18) P. Cuff, E. Song, “The Likelihood Encoder for Source Coding,” Proc. of IEEE Inf. Theory Workshop (ITW), Sept., 2013.
19) S. Satpathy and P. Cuff, “Secure Cascade Channel Synthesis,” Proc. of IEEE Int’l. Symp. on Inf. Theory (ISIT), July, 2013.
20) E. Song, P. Cuff, V. Poor, “A Bit of Secrecy for Gaussian Source Compression,” Proc. of IEEE Int’l. Symp. on Inf. Theory (ISIT), July, 2013.
21) C. Schieler and P. Cuff, “Rate-Distortion Theory for Secrecy Systems,” Proc. of IEEE Int’l. Symp. on Inf. Theory (ISIT), July, 2013.
22) S. Shang, P. Cuff, P. Hui, and S. Kulkarni, “An Upper Bound on the Convergence Time for Quantized Consensus,” Proceedings of IEEE INFOCOM, April, 2013.
23) P. Cuff, “Optimal Equivocation in Secrecy Systems – A Special Case of Distortion-based Characterization,” Proc. of the Information Theory and Applications Workshop (ITA), February, 2013.
24) C. Schieler, E. Song, P. Cuff, and V. Poor, “Source-Channel Secrecy with Causal Disclosure,” Proc. of the Allerton Conference on Communication, Control, and Computing, Oct. 2012.
25) T. Wang, J. Sturm, P. Cuff, S. Kulkarni, “Condorcet Voting Methods Avoid the Paradoxes of Voting Theory,” Proc. of the Allerton Conference on Communication, Control, and Computing, Oct. 2012.
26) S. Shang, S. Kulkarni, P. Cuff, P. Hui, “A Random Walk Based Model Incorporating Social Information for Recommendations,” Proc. of the IEEE Machine Learning for Signal Processing Workshop, September, 2012.
27) C. Schieler and P. Cuff, “Secrecy is Cheap if the Adversary Must Reconstruct,” Proc. of IEEE Int’l. Symp. on Inf. Theory (ISIT), July, 2012.
28) S. Shang, P. Cuff, S. Kulkarni, and P. Hui, “An Upper Bound on the Convergence Time for Distributed Binary Consensus,” Proc. of the Int’l. Conf. on Information Fusion, July, 2012.

Changes in research objectives (if any):

Change in AFOSR Program Manager, if any:

Extensions granted or milestones slipped, if any:

AFOSR LRIR Number

LRIR Title

Reporting Period

Laboratory Task Manager

Program Officer

Research Objectives

Technical Summary

Funding Summary by Cost Category (by FY, $K)

	Starting FY	FY+1	FY+2
Salary			
Equipment/Facilities			
Supplies			
Total			

Report Document

Report Document - Text Analysis

Report Document - Text Analysis

Appendix Documents

2. Thank You

E-mail user

May 26, 2015 15:35:46 Success: Email Sent to: cuff@princeton.edu